

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-67256

(P2003-67256A)

(43) 公開日 平成15年3月7日(2003.3.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 M 5 B 0 6 5
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A 5 J 1 0 4
			6 0 1 E

審査請求 未請求 請求項の数 5 O L (全 24 頁)

(21) 出願番号 特願2001-252399(P2001-252399)

(22) 出願日 平成13年8月23日(2001.8.23)

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番  
1号

(72) 発明者 岡田 佳之

神奈川県川崎市中原区上小田中4丁目1番  
1号 富士通株式会社内

(74) 代理人 100092978

弁理士 真田 有

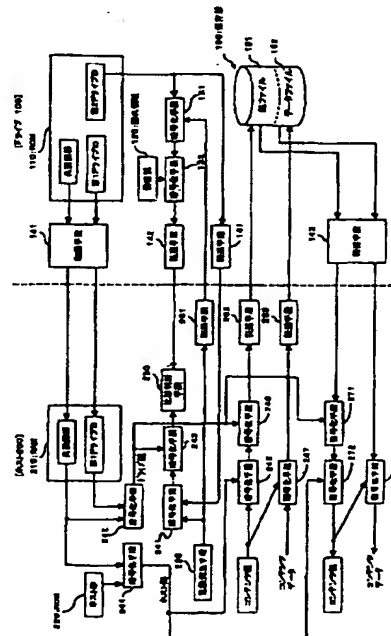
最終頁に続く

(54) 【発明の名称】 データ保護方法

(57) 【要約】

【課題】ドライブ側での処理の負荷が大きくなることなく、ドライブのデータを不正なアクセスから保護し、ドライブ側での不正コピーのみならずホスト側での不正行為も確実に防止し、著作権を確実に保護できるようにするとともに、ドライブの不正転用も確実に防止できるようにする。

【解決手段】ホスト200においてドライブ100の認証を行ない、ドライブ100が認証された場合、ホスト200の記憶領域220に予め登録されているホストIDとドライブ100の記憶領域110から読み出された共通鍵および第1識別情報とによりコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をドライブ100へ転送するとともに、ホスト200においてドライブ100に記録・保存すべきコンテンツデータをコンテンツ鍵により暗号化し、暗号化されたコンテンツデータをドライブ100へ転送する。



## 【特許請求の範囲】

【請求項1】 データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該アクセス装置において該データ記録装置の認証を行なうステップと、

該データ記録装置が認証された場合、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化するステップと、

暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、

該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、

暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【請求項2】 データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置に、コンテンツ鍵により暗号化されたコンテンツデータを書き込むとともに、所定のアクセス装置識別情報と該データ記録装置の記憶領域に予め登録されている共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込むステップと、

該アクセス装置において該データ記録装置の認証を行なうステップと、

該データ記録装置が認証された場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、

該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、

復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとを含むことを特徴とする、データ保護方法。

【請求項3】 データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装

置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、1回のみ書き込み可能な記憶領域に書き込むステップと、

以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記1回のみ書き込み可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、

該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報によりコンテンツ鍵を暗号化するステップと、

暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、

該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、

暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【請求項4】 該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、

該アクセス装置において、該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報により、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとをさらに含むことを特徴とする、請求項3記載のデータ保護方法。

【請求項5】 該アクセス装置の認証を行なうステップが、

該データ記録装置で乱数を発生するステップと、

該乱数を該データ記録装置から該アクセス装置へ転送するステップと、

該データ記録装置において、該アクセス装置識別情報を前記乱数により暗号化するステップと、

該アクセス装置において、該アクセス装置識別情報を該データ記録装置からの前記乱数により暗号化するステップと、

暗号化された該アクセス装置識別情報を該アクセス装置から該データ記録装置へ転送するステップと、

該アクセス装置からの前記暗号化されたアクセス装置識

別情報と該データ記録装置で暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断するステップとを含み、

これらのアクセス装置識別情報が一致すると判断された場合、該アクセス装置が認証されることを特徴とする、請求項3または請求項4に記載のデータ保護方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データを記録・保存するデータ記録装置と、このデータ記録装置にアクセスするアクセス装置との間で音楽や映像などのデータを転送する際に、不正なアクセスからデータを保護するための方法に関する。ここで、データ記録装置は、例えば、音楽や映像などのデータを記録するデジタル録画再生装置であり、アクセス装置は、例えば、パーソナルコンピュータや、データ記録装置内のホスト（CPU）である。

【0002】近年、パソコンの性能向上やMPEG2-ISOの出現で映像、音楽のデータを取り扱うことが容易になってきている。また、数10GB（ギガバイト）の大容量ディスクが安価に手に入るようになり、ハードディスクドライブ（HDD）あるいは光ディスクドライブをベースにした、新しいデジタル録画再生装置も登場してきている。

【0003】このように安価で高性能のデータ記録装置を一般に広く普及させる際の鍵となるのが、そのデータ記録装置によって記録される各種データ（コンテンツ）の著作権の保護であり、不正コピーなどを確実に防止してコンテンツ提供者の権利を守る必要がある。本発明では、ホスト（アクセス装置）とドライブ（データ記録装置）との間でデータを転送する際、特に、ドライブ側に処理負担をかけることなく、データを不正なアクセスから保護し、著作権を確実に保護できるようにした技術を提供する。

【0004】

【従来の技術】現状のデジタル録画再生装置としては、HDDレコーダや蓄積型セットトップボックス（STB）などがあるが、著作権保護の関係から、その装置に内蔵されたHDDを、装置外へ取り出せないように機構的に固定化する立場が採られる場合が多い。一方、ユーザの立場からすれば、装置（HDD以外の部分）はそのままにしながら、HDDの部分だけを、近年、容量が急激に増大しているPC（Personal Computer）系の新型HDDに置き換えたいという要望が強い。

【0005】その際、ホストとディスクドライブとの間のデータ転送時における著作権保護（つまり、不正なアクセスからのデータ保護）が課題となる。従来、PC系の標準インタフェース（ATA/ATAPI：Advanced Technologies Attachment/ATA Packet Interface）を利用した著作権保護方法（データ保護方法）とし

ては、CPPM（Content Protection for Pre-recorded Media）やCPRM（Content Protection for Recordable Media）が知られている。

【0006】CPRMでは、ドライブ内にドライブ固有のID（識別情報；媒体で言えばメディアID）が設定されており、ホストからディスクに対するコンテンツデータの書込は、以下のような手順（ステップ(a1)～(a8)）で行なわれる。

(a1)ホストからドライブに対して、ドライブ内のROM領域に保存されている共通鍵群（複数のメディアキーブロック、複数の秘密鍵）および第1ドライブID（静的なID）の転送を要求する。

【0007】(a2)ステップ(a1)の要求に応じて、共通鍵群および第1ドライブIDをドライブからホストへ転送する。

(a3)ホストのRAM領域に、ドライブからの共通鍵群および第1ドライブIDを格納する。

(a4)ホスト側で生成した乱数をドライブへ送るとともに、ホストからドライブに対して、生の第2ドライブID（動的なID）と、暗号化された第2ドライブIDとの転送を要求する。

【0008】(a5)ステップ(a4)の要求に応じて、第2ドライブIDを、ホストからの乱数と、隠れ領域に既に書き込まれているドライブ鍵（秘密鍵）とにより暗号化し、生の第2ドライブIDと暗号化された第2ドライブIDとをドライブからホストへ転送する。

【0009】(a6)ホストにおいて、ステップ(a3)で保存した共通鍵群および第1ドライブIDからドライブ鍵（相当）を作成し、そのドライブ鍵とステップ(a4)で生成した乱数とにより、ドライブからの生の第2ドライブIDを暗号化してから、ホスト側で暗号化された第2ドライブIDと、ドライブからの暗号化された第2ドライブIDとを比較し、これらが一致するか否かを判断する。

【0010】(a7)ステップ(a6)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ドライブに書き込むべきコンテンツデータをコンテンツ鍵により暗号化するとともに、共通鍵群および第1ドライブIDから作成されたドライブ鍵（相当）によりコンテンツ鍵を暗号化する。そして、暗号化されたコンテンツデータおよび暗号化されたコンテンツ鍵を、ホストからドライブへ転送しディスクに書き込む。

(a8)ステップ(a6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、コンテンツデータをドライブに転送することなく処理を中断する。

【0011】一方、CPRMでは、上述のごとくディスクに書き込まれたコンテンツデータをディスクからホストへ読み出す際、上述と同様の手順（ステップ(a1)～(a6)）でドライブの認証を行なった後、以下のような手順（ステップ(b1)および(b2)）でコンテンツデータが読み

出される。

(b1)ステップ(a6)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ホストは、ドライブ(ディスク)から、暗号化されたコンテンツ鍵および暗号化されたコンテンツデータを読み出す。そして、共通鍵群および第1ドライブIDから作成されたドライブ鍵(相当)により、暗号化されたコンテンツ鍵を復号化してから、さらに、復号化されたコンテンツ鍵により、暗号化されたコンテンツデータを復号化する。

【0012】(b2)ステップ(a6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、コンテンツをディスクから読み出すことなく処理を中断する。なお、CPRMは、読出し専用の著作権保護方式であり、このCPRMでは、上述したステップ(a1)~(a6)、(b1)および(b2)が実行される。

【0013】上述したドライブ認証手順[ステップ(a1)~(a6)]は、チャレンジ&レスポンス方式と呼ばれ、CPRMやCPRMでは、ホスト側のみで認証が行なわれている。つまり、単方向のドライブ認証が行なわれ、これにより、ドライブ側での処理の負担を軽減している。また、コンテンツ鍵やコンテンツデータがドライブ固有のIDに基づいてディスクに記録されているので、そのドライブのディスクに記録されたデータが別の媒体に不正にコピー(ボリュームコピー)されたとしても、データ読出に際してIDが一致しないため、不正コピーされたデータを読み出すことはできない。従って、CPRMやCPRMは不正コピーの防止に有効である。

【0014】CPRMやCPRM以外の著作権保護手法の代表的なものとしては、IEEE1394-1Fを利用したDTCP(Digital Transmission Content Protection)がある。このDTCPは、装置間のデータ転送を想定しており、相互認証を基本としている。このDTCPとしては、フル認証(Full Authentication)方式と制限認証(Restrict Authentication)方式との2種類がある。フル認証方式では、公開鍵/秘密鍵暗号技術の電子署名アルゴリズムとDH鍵交換アルゴリズムとが採用されており、いずれのアルゴリズムも楕円曲線暗号を基礎としている。

【0015】ここで、ホストとディスクドライブとの間のデータ転送に際しフル認証方式のDTCPを用いた場合の、相互認証手順[ステップ(c1)~(c9)]について説明する。

(c1)ホストからドライブに対し、ホストの認証を要求する。このとき、ホストは、ドライブに乱数とホスト固有IDとを送る。このホスト固有IDは、DTCPのライセンス組織(米国DTLA社)が機器毎に生成した証明情報であり、公開鍵や電子署名なども含まれる。

【0016】(c2)ドライブは、ホストから乱数とホスト固有IDとを受け取ると、ホスト固有IDがDTLA社作成の情報であることを、電子署名の検証処理に従って確

認するとともに、そのホスト固有IDがドライブ側で保持される不正機器リストに載っていないかを調べる。

(c3)ステップ(c2)での確認の結果、何ら問題がなければ、ドライブからホストに対し、ドライブの認証を要求する。このとき、ドライブは、ホストに乱数とドライブ固有IDを送る。このドライブ固有IDも、ホスト固有IDと同様、米国DTLA社が機器毎に生成した証明情報である。

【0017】(c4)ホストは、ドライブから乱数とドライブ固有IDとを受け取ると、ステップ(c2)と同様、ドライブ固有IDがDTLA社作成の情報であることを、電子署名の検証処理に従って確認するとともに、そのドライブ固有IDがホスト側で保持される不正機器リストに載っていないかを調べる。

(c5)ステップ(c4)での確認の結果、何ら問題がなければ、DH鍵交換方式(配送・共有方式)に従い、暗号鍵を共有するため、各装置(ホスト/ドライブ)において、その装置のDH情報を計算する。

【0018】(c6)ホストからドライブへ、ホストのDH情報を送る。

(c7)ドライブは、ホストから受け取ったDH情報が間違いなくホストから送られてきたデータであることを、電子署名の検証に従って確認する。

(c8)逆に、ドライブからホストへ、ドライブのDH情報を送る。

(c9)ホストは、ドライブから受け取ったDH情報が間違いなくドライブから送られてきたデータであることを、電子署名の検証に従って確認する。

【0019】上述のように、DTCPに代表される相互認証方式においては、ホストおよびドライブが、それぞれ、ドライブおよびホストがデータ転送を行なうのに正しい相手であるかどうかをチェックする機構(相互認証機構)を有しているので、ドライブ側での不正コピーが確実に防止されるだけでなく、ホスト側での不正行為(成りすまし等)も確実に防止することができる。

【0020】なお、制限認証方式のDTCPは、共通の秘密鍵とハッシュ関数とを用いて認証を行なうものであるが、この制限認証方式のDTCPにおいても、基本的には上述したフル認証方式のDTCPと同様、ホストとドライブとは、対等な関係であり、相互に同様の認証処理を実行するので、その説明は省略する。

【0021】

【発明が解決しようとする課題】しかしながら、上述したCPRMやCPRMでは、ホスト側でドライブの認証を行なうだけなので、ドライブ側での不正コピーを確実に防止することはできないが、ドライブ側でホストの認証を行なうことができない。従って、ドライブの認証が成立すれば、複数の装置(ホスト)から、つまり、正規ではないホストからも、そのドライブにアクセスし、ディスクに記録されたコンテンツデータを再生することが可

能になってしまう。このため、ドライブのデータを、正規ではないホストによる不正なアクセスから保護できず、ホスト側での不正行為（成りすまし等）を防止することができないという課題がある。

【0022】そこで、上述したDTCPを採用することにより、ホスト側でドライブの認証が行なわれ且つドライブ側でホストの認証が行なわれるので、ドライブ側での不正コピーもホスト側での不正行為も防止することは可能になる。しかし、上述のごとくDTCPの認証処理は極めて複雑であり、ホストとドライブとが対等な関係であるため、特に、ドライブ側で複雑な認証処理を行なわなければならない、ドライブ側での処理の負荷が大きくなり好ましくない。

【0023】また、近年、セットトップボックス（STB）を安価に貸し出すというビジネスが展開され始めているが、このようなビジネスの展開に伴い、STB内のハードディスクドライブに記録されたデータを不正コピーするだけでなく、そのハードディスクドライブそのものを抜き出してパソコンのドライブとして不正転用するという、不正利用者が出現してきている。

【0024】このような不正利用者に対抗するために、上述したDTCPのような相互認証方式を採用することが望まれている。しかし、DTCPでは、上述した通り、DTCPの認証処理は極めて複雑で、ドライブ側での処理の負荷が大きくなる。このため、より簡易な処理で、且つ、ドライブ側での負荷を大きくすることなく、上述のような不正転用を確実に防止できるようにすることが望まれている。

【0025】本発明は、このような課題に鑑み創案されたもので、ドライブ側での処理の負荷を大きくすることなく、データを不正なアクセスから保護し、データ記録装置（ドライブ）側での不正コピーのみならずアクセス装置（ホスト）側での不正行為をも確実に防止し、著作権を確実に保護できるようにするとともに、データ記録装置の不正転用も確実に防止できるようにした、データ保護方法を提供することを目的とする。

【0026】

【課題を解決するための手段】上記目的を達成するために、本発明のデータ保護方法（請求項1）は、データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とによりコンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を該データ記録装置に書き込むべく該アクセス装置から該データ記録装置へ転送

するステップと、該アクセス装置において該データ記録装置に記録・保存すべきコンテンツデータを該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを該データ記録装置に書き込むべく該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴としている。

【0027】また、本発明のデータ保護方法（請求項2）は、データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置に、コンテンツ鍵により暗号化されたコンテンツデータを書き込むとともに、所定のアクセス装置識別情報と該データ記録装置の記憶領域に予め登録されている共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込むステップと、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとを含むことを特徴としている。

【0028】さらに、本発明のデータ保護方法（請求項3）は、データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、1回のみ書き込み可能な記憶領域に書き込むステップと、以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記1回のみ書き込み可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報によりコンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装

置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴としている。

【0029】このとき、該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報により、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとがさらに含まれていてもよい（請求項4）。

【0030】また、該アクセス装置の認証を行なうステップが、該データ記録装置で乱数を発生するステップと、該乱数を該データ記録装置から該アクセス装置へ転送するステップと、該データ記録装置において、該アクセス装置識別情報を前記乱数により暗号化するステップと、該アクセス装置において、該アクセス装置識別情報を該データ記録装置からの前記乱数により暗号化するステップと、暗号化された該アクセス装置識別情報を該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置からの前記暗号化されたアクセス装置識別情報と該データ記録装置で暗号化されたアクセス装置識別情報とを比較し、一致するかどうかを判断するステップとを含み、これらのアクセス装置識別情報が一致すると判断された場合に該アクセス装置を認証するように構成してもよい（請求項5）。

【0031】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

（1）第1実施形態の説明

図1は本発明の第1実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図であり、第1実施形態におけるデータ保護システムは、図1に示すように、データを記録・保存するデータ記録装置としてのドライブ（例えばHDD）100と、このドライブ100にアクセスするアクセス装置としてのホスト（例えばCPU）200との間でデータ転送を行なう際に、ドライブ100のデータを不正なアクセスから保護するためのものである。

【0032】ドライブ100は、ROM110、隠れ領域120、暗号化手段131、132、転送手段141～143および保存部150をそなえて構成されてい

る。ここで、ROM（Read Only Memory；第1記憶領域）110は、共通鍵群、第1ドライブID（第1識別情報）および第2ドライブID（第2識別情報）を予め登録されて保持するものであり、隠れ領域120は、ドライブ鍵（秘密鍵）を予め登録されて保持するものである。

【0033】暗号化手段131は、ROM110から読み出された第2ドライブIDを、ホスト200からの乱数により暗号化するものであり、暗号化手段132は、暗号化手段131による暗号化結果を、さらに、隠れ領域から読み出されたドライブ鍵（秘密鍵）により暗号化するものである。これらの暗号化手段131および132が、ホスト200からの要求に応じて、第2ドライブIDを、当該要求とともにホスト200から送られてくる乱数とドライブ100のドライブ鍵（秘密鍵）とにより暗号化する第1暗号化手段として機能することになる。

【0034】転送手段（第1転送手段）141は、ホスト200からの要求に応じて、共通鍵群、第1ドライブIDおよび第2ドライブIDをROM110から読み出してホスト200へ転送するものである。転送手段（第2転送手段）142は、暗号化手段131および132により暗号化された第2ドライブIDをホスト200へ転送するものである。転送手段（第3転送手段）143は、ホスト200からの要求に応じて、暗号化コンテンツデータおよび暗号化コンテンツ鍵を保存部150から読み出してホスト200へ転送するものである。

【0035】保存部150は、ドライブ100におけるディスク媒体そのものであり、ホスト200からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存するもので、コンテンツ鍵を保存する鍵ファイル151と、コンテンツデータを保存するデータファイル152とを有している。なお、保存部150に保存されるコンテンツデータは、コンテンツ鍵により暗号化されているとともに、保存部150に保存されるコンテンツ鍵は、後述するごとく、ホストID（所定のアクセス装置識別情報）とドライブ100の共通鍵および第1ドライブIDとにより暗号化されている。

【0036】一方、ホスト200は、RAM210、ROM220、乱数発生手段230、暗号化手段241～247、比較判断手段250、転送手段261～263および復号化手段271～273をそなえて構成されている。ここで、RAM（Random Access Memory）210は、ドライブ100から転送されてきた共通鍵群および第1ドライブIDを一時的に保存するものであり、ROM（Read Only Memory；第2記憶領域）220は、ホスト200固有の識別情報であるホストID（アクセス装置識別情報）を予め登録されて保持するものである。

【0037】乱数発生手段（第1乱数発生手段）230は、ホスト200がドライブ100に対してアクセスす

る際に乱数を発生するものである。暗号化手段241は、ドライブ100から転送されてきた生の第2ドライブIDを、乱数発生手段230で生成された乱数により暗号化するものであり、暗号化手段242は、RAM210に保存された第1ドライブIDを、RAM210に保存された共通鍵群により暗号化することによって、ドライブ鍵（相当）を生成・出力するものであり、暗号化手段243は、暗号化手段241による暗号化結果を、さらに、暗号化手段242からのドライブ鍵（相当）により暗号化するものである。

【0038】これらの暗号化手段241～243が、ドライブ100のROM110から読み出された第2ドライブIDを、乱数発生手段230で発生された乱数と、ドライブ100のROM110から読み出された共通鍵群および第1ドライブIDとにより暗号化する第2暗号化手段として機能することになる。比較判断手段（第1比較判断手段）250は、ドライブ100から転送手段142を通じて転送されてくる、暗号化された第2ドライブIDと、暗号化手段241～243によって暗号化された第2ドライブIDとを比較し、一致するか否かを判断するものである。

【0039】そして、ホスト200がドライブ100（保存部150）にコンテンツデータを記録・保存する際、比較判断手段250により2種類の第2ドライブIDが一致すると判断された場合に、後述する暗号化手段244～247および転送手段261～263が動作するようになっている。また、ホスト200がドライブ100（保存部150）からコンテンツデータを読み出す際、比較判断手段250により2種類の第2ドライブIDが一致すると判断された場合に、後述する復号化手段271～273が動作するようになっている。

【0040】暗号化手段244は、ROM220に保存されたホストIDを、RAM210に保存された共通鍵群により暗号化することによって、ホスト鍵を生成・出力するものであり、暗号化手段245は、コンテンツ鍵を、暗号化手段244の暗号化結果であるホスト鍵により暗号化するものであり、暗号化手段246は、暗号化手段245の暗号化結果を、さらに、暗号化手段242からのドライブ鍵（相当）により暗号化するものである。

【0041】2種類の第2ドライブIDが一致すると比較判断手段250が判断した場合、上述した暗号化手段244～246および暗号化手段242が、ROM220から読み出されたホストIDと、RAM210に保存されている共通鍵群および第1ドライブIDとにより、コンテンツ鍵を暗号化する第3暗号化手段として機能することになる。

【0042】暗号化手段（第4暗号化手段）247は、ドライブ100に記録・保存すべきコンテンツデータを、コンテンツ鍵により暗号化するものである。転送手

段（第4転送手段）261は、乱数発生手段230で発生された乱数をドライブ100（暗号化手段131）へ転送するものである。

【0043】転送手段（第5転送手段）262は、暗号化手段242および244～246により暗号化されたコンテンツ鍵を、ドライブ100の保存部150（鍵ファイル151）に書き込むべく、ドライブ100へ転送するものである。転送手段（第6転送手段）263は、暗号化手段247により暗号化されたコンテンツデータを、ドライブ100の保存部150（データファイル152）に書き込むべく、ドライブ100へ転送するものである。

【0044】復号化手段271は、ドライブ100の保存部150（鍵ファイル151）から読み出された暗号化コンテンツ鍵を、暗号化手段242からのドライブ鍵（相当）により復号化するものであり、復号化手段272は、復号化手段271による復号化結果を、さらに、暗号化手段244からのホスト鍵により復号化するものである。

【0045】2種類の第2ドライブIDが一致すると比較判断手段250が判断した場合、上述した復号化手段271および272が、ROM220から読み出されたホストIDと、RAM210に保存されている共通鍵群および第1ドライブIDとにより、ドライブ100の保存部150（鍵ファイル151）から読み出された暗号化コンテンツ鍵を復号化する第1復号化手段として機能することになる。

【0046】復号化手段（第2復号化手段）273は、復号化手段271および272により復号化されたコンテンツ鍵により、ドライブ100の保存部150（データファイル152）から読み出された暗号化コンテンツデータを復号化するものである。

【0047】上述したホスト200における乱数発生手段230、暗号化手段241～247、比較判断手段250、転送手段261～263および復号化手段271～273としての機能は、専用ソフトウェア（アクセスプログラム）によって実現される。このアクセスプログラムは、例えばフレキシブルディスク、CD-ROM等のコンピュータ読取可能な記録媒体に記録された形態で提供される。第1実施形態においては、ホスト200を成すROM（Read Only Memory）等に予めアクセスプログラムを格納しておき、このアクセスプログラムを、ホスト200を成すCPUによって読み出し実行することで、上述した乱数発生手段230、暗号化手段241～247、比較判断手段250、転送手段261～263および復号化手段271～273としての機能が実現される。なお、アクセスプログラムは、例えば磁気ディスク、光ディスク、光磁気ディスク等の記憶装置（記録媒体）に記録しておき、その記憶装置から通信経路を介してコンピュータに提供されてもよい。また、ドライブ1



00における暗号化手段131、132および転送手段141、142としての機能も、専用ソフトウェアによって実現される。

【0048】なお、ドライブ100においては、ドライブ100からホスト200へ転送するデータの種類毎に、転送手段141~143をそなえているが、実際には、これらの転送手段141~143としての機能を一つの転送手段によって実現してもよい。また、暗号化手段131および132としての機能も一つの暗号化手段によって実現してもよい。

【0049】同様に、ホスト200においては、ホスト200からドライブ100へ転送するデータの種類毎に、転送手段261~263をそなえているが、実際には、これらの転送手段261~263としての機能を一つの転送手段によって実現してもよい。また、暗号化手段241~247としての機能も一つの暗号化手段によって実現してもよいし、復号化手段271~273としての機能も一つの復号化手段によって実現してもよい。

【0050】次に、上述のごとく構成された第1実施形態のデータ保護システムの動作について、図2~図5を参照しながら説明する。なお、図2は第1実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図、図3は第1実施形態におけるコンテンツデータ書込手順を説明するための図、図4は第1実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図、図5は第1実施形態におけるコンテンツデータ読出手順を説明するための図である。

【0051】第1実施形態では、前述したCPRMの手法を用いながら、コンテンツデータおよびコンテンツ鍵を書き込む際に、コンテンツ鍵をホスト固有のIDを用いて暗号化している。つまり、第1実施形態では、ドライブ100内にドライブ固有の第1ドライブIDおよび第2ドライブIDが設定されるとともに、ホスト200内にホスト固有のホストIDが設定されており、ホスト200からドライブ100（保存部150）に対するコンテンツデータの書込は、以下のような手順（ステップ(A1)~(A11)）で行なわれる。なお、図2および図3においては、ステップ(A1)~(A11)に対応する処理を行なっている箇所に、それぞれ(A1)~(A11)が符号として記入されている。

【0052】(A1)ホスト200からドライブ100に対して、ドライブ100内のROM110領域に保存されている共通鍵群（複数のメディアキーブロック、複数の秘密鍵）および第1ドライブID（静的なID）の転送を要求する。

(A2)ステップ(A1)の要求に応じて、共通鍵群および第1ドライブIDを、ROM110から読み出し、ドライブ100からホスト200へ転送する（図1の転送手段141の機能）。

【0053】(A3)ホスト200のRAM210に、ドライブ100からの共通鍵群および第1ドライブIDを格納・保持する。

(A4)ホスト200側の乱数発生手段230で乱数を発生し、その乱数をドライブ100へ送るとともに（図1の転送手段261の機能）、ホスト200からドライブ100に対して、生の第2ドライブID（動的なID）とその第2ドライブIDを上記乱数により暗号化したものごとを転送するように要求する。

【0054】(A5)ステップ(A4)の要求に応じて、暗号化手段131および132が、第2ドライブIDを、ホスト200からの乱数と、隠れ領域120に書き込まれているドライブ鍵（秘密鍵）とにより暗号化する。そして、生の第2ドライブIDと暗号化された第2ドライブIDとをドライブ100からホスト200へ転送する（図1の転送手段141、142の機能）。

【0055】(A6)ホスト200において、暗号化手段242が、ステップ(A3)で保存した共通鍵群と第1ドライブIDとに基づきドライブ鍵（相当）を作成し、そのドライブ鍵とステップ(A4)で生成した乱数とにより、ドライブ100からの生の第2ドライブIDを暗号化する。そして、比較判断手段250において、ホスト200側で暗号化された第2ドライブIDと、ドライブ100からの暗号化された第2ドライブIDとを比較し、これらが一致するか否かを判断する。第1実施形態では、上記ステップ(A1)~(A6)により、ドライブ100の認証がホスト200側で行なわれる。

【0056】(A7)ステップ(A6)で一致したと判断された場合には、ドライブ100の認証に成功したものと判断し、暗号化手段242および244~246が、ROM220から読み出されたホストIDと、RAM210に保存されている共通鍵群および第1ドライブIDとにより、コンテンツ鍵を暗号化する。つまり、ホストIDと共通鍵群とから生成されたホスト鍵と、第1ドライブIDと共通鍵群とから生成されたドライブ鍵（相当）とによって、コンテンツ鍵が暗号化される。

【0057】(A8)ステップ(A7)で暗号化されたコンテンツ鍵を、ホスト200からドライブ100へ転送し（図1の転送手段262の機能）、ドライブ100の保存部150（鍵ファイル151）に書き込む。

(A9)ステップ(A6)で一致したと判断された場合、上述したステップ(A7)、(A8)の処理と並行して、暗号化手段247が、ドライブ100に書き込むべきコンテンツデータをコンテンツ鍵により暗号化する。

【0058】(A10)ステップ(A9)で暗号化されたコンテンツデータを、ホスト200からドライブ100へ転送し（図1の転送手段263の機能）、ドライブ100の保存部150（データファイル152）に書き込む。

(A11)ステップ(A6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したス



ステップ(A7)～(A10)の処理を行なうことなく、処理を中断する。

【0059】一方、上述のごとくドライブ100の保存部150に書き込まれたコンテンツデータをドライブ100からホスト200へ読み出す際、第1実施形態では、上述と同様のステップ(A1)～(A6)に従ってドライブ100の認証を行なった後、以下のような手順【ステップ(B1)～(B6)】でコンテンツデータが読み出される。なお、図4および図5においては、ステップ(A1)～(A6)および(B1)～(B5)に対応する処理を行なっている箇所に、それぞれ(A1)～(A6)および(B1)～(B5)が符号として記入されている。ここで、ステップ(A1)～(A6)によるドライブ認証手順は上述と同様であるので、その説明は省略する。

【0060】(B1)ステップ(A6)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ホスト200は、ドライブ100に対し、暗号化コンテンツ鍵および暗号化コンテンツデータの読出を要求する。(B2)ステップ(B1)の要求に応じて、ドライブ100は、暗号化コンテンツ鍵および暗号化コンテンツを保存部150から読み出してホスト200へ転送する(図1の転送手段143の機能)。

【0061】(B3)ホスト200においては、復号化手段271および272が、ROM220から読み出されたホストIDと、RAM210に保存されている共通鍵群および第1ドライブIDとにより、ドライブ100の保存部150(鍵ファイル151)から読み出された暗号化コンテンツ鍵を復号化する。つまり、ホストIDと共通鍵群とから生成されたホスト鍵と、第1ドライブIDと共通鍵群とから生成されたドライブ鍵(相当)とによって、暗号化されたコンテンツ鍵が復号化される。

【0062】(B4)そして、復号化手段273が、復号化手段271および272で復号化されたコンテンツ鍵により、ドライブ100の保存部150(データファイル152)から読み出された暗号化コンテンツデータを復号化する。

(B5)ステップ(A6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したステップ(B1)～(B4)の処理を行なうことなく、処理を中断する。

【0063】(B6)コンテンツ鍵を暗号化してドライブ100に書き込んだホスト200とは異なるホストが、コンテンツ鍵を復号化しようとした場合、復号化に用いられるホストIDが、暗号化に用いられたホストIDとは異なってしまう。このような場合、ステップ(B3)において正しいコンテンツ鍵が復元されないので、ステップ(B4)において暗号化コンテンツデータを復号化することができず、ホスト200は、本来のコンテンツデータを得ることができなくなる。

【0064】このように、本発明の第1実施形態として

のデータ保護システムによれば、ホスト200がコンテンツデータおよびコンテンツ鍵をドライブ100に書き込む際に、コンテンツ鍵が、ドライブ100の識別情報(第1ドライブID)にホストIDの要素を加えて暗号化されているので、コンテンツデータやコンテンツ鍵をドライブ100に書き込んだ正規のホスト200しか、そのコンテンツデータを読み出すことができない。

【0065】つまり、正規のホスト200以外のホスト(CPU等)がドライブ100からコンテンツデータを読み出しても、そのホストの識別情報(ホストID)が正規のものと異なっているため、コンテンツ鍵を正しく復号化することができないので、コンテンツデータを正しく復号化できず、コンテンツデータを読み出すことができなくなる。

【0066】従って、CPPMやCPRM等の単方向認証を採用してドライブ100側での処理の負荷を大きくすることなく、ホスト200とドライブ100とを1対1で対応させる専用接続の形態が実現され、ドライブ100のデータを不正なアクセスから保護することができるので、ドライブ100側での不正コピーのみならず、ホスト200側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【0067】〔2〕第2実施形態の説明

図6は本発明の第2実施形態としてのデータ保護方法を適用されたデータ保護システム(アクセス装置およびデータ記録装置)の機能構成を示すブロック図であり、第2実施形態におけるデータ保護システムも、第1実施形態とほぼ同様に構成されているが、図6に示すように、第2実施形態におけるデータ保護システムのドライブ(データ記録装置)100Aは、第1実施形態のドライブ100に、暗号化手段133、転送手段144、1回書き込み可能記憶領域160、乱数発生手段170および比較判断手段180をさらにそなえて構成されている。また、第2実施形態におけるデータ保護システムのホスト(アクセス装置)200Aは、第1実施形態のホスト200に、暗号化手段248、転送手段264および転送手段265をさらにそなえて構成されている。なお、図中、既述の符号と同一の符号は、同一もしくはほぼ同一の部分を示しているため、その説明は省略する。

【0068】ここで、ドライブ100Aにおいて、1回書き込み可能記憶領域160は、ドライブ100Aが初期状態の時にこのドライブ100Aに最初に接続されたホスト200AのホストIDを書き込まれるもので、データを1回だけ書き込むことができる領域である。乱数発生手段(第2乱数発生手段)170は、ホスト200Aからアクセスされる都度、乱数を発生するものである。

【0069】転送手段(第7転送手段)144は、乱数発生手段170で発生された乱数をホスト200Aへ転送するものである。暗号化手段(第5暗号化手段)13

3は、1回書き込み可能記憶領域160から読み出されたホストIDを、乱数発生手段170で発生された乱数により暗号化するものである。

【0070】比較判断手段(第2比較判断手段)180は、暗号化手段133で暗号化されたホストIDと、後述のごとくホスト200Aから転送されてきた暗号化ホストIDとを比較し、一致するか否かを判断するものである。一方、ホスト200Aにおいて、暗号化手段(第6暗号化手段)248は、ROM220に保存されているホストIDを、ドライブ100Aから転送手段144を通じて送られてくる乱数により暗号化するものである。

【0071】転送手段(第8転送手段)264は、初期状態のドライブ100Aに最初に接続された時に、ホストIDをドライブ100Aの1回書き込み可能記憶領域160に書き込むべく、ホストIDをROM220から読み出してドライブ100Aへ転送するものである。転送手段(第9転送手段)265は、ホスト200Aがドライブ100Aにアクセスする都度、暗号化手段248により暗号化されたホストIDをドライブ100A(比較判断手段180)へ転送するものである。

【0072】そして、第2実施形態のデータ保護システムにおいては、ホスト200Aがドライブ100A(保存部150)にコンテンツデータを記録・保存する際、比較判断手段250および180がいずれも識別情報が一致すると判断した場合に、暗号化手段242、244~247、転送手段262および263が動作するようになっている。また、ホスト200Aがドライブ100A(保存部150)からコンテンツデータを読み出す際、比較判断手段250により2種類の第2ドライブIDが一致すると判断された場合に、後述する復号化手段271~273が動作するようになっている。

【0073】上述のごとく第2実施形態のドライブ100Aにおいて新たに追加された、暗号化手段133、転送手段144、乱数発生手段170および比較判断手段180としての機能も、専用ソフトウェアによって実現される。同様に、第2実施形態のホスト200Aにおいて新たに追加された、暗号化手段248、転送手段264および転送手段265としての機能も、専用ソフトウェア(アクセスプログラム)によって実現される。

【0074】なお、ドライブ100Aにおいては、転送手段144としての機能を、第1実施形態で説明した転送手段141~143としての機能とともに、一つの転送手段によって実現してもよい。また、暗号化手段133としての機能を、第1実施形態で説明した暗号化手段131および132としての機能とともに、一つの暗号化手段によって実現してもよい。

【0075】同様に、ホスト200Aにおいては、転送手段264および265としての機能を、第1実施形態で説明した転送手段261~263としての機能とも

に、一つの転送手段によって実現してもよい。また、暗号化手段248としての機能を、第1実施形態で説明した暗号化手段241~247としての機能とともに、一つの暗号化手段によって実現してもよい。

【0076】次に、上述のごとく構成された第2実施形態のデータ保護システムの動作について、図7~図10を参照しながら説明する。なお、図7は第2実施形態のデータ保護システムにおけるコンテンツデータ書き込み動作に係る要部を取り出して示すブロック図、図8は第2実施形態におけるコンテンツデータ書き込み手順を説明するための図、図9は第2実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図、図10は第2実施形態におけるコンテンツデータ読出手順を説明するための図である。

【0077】第2実施形態では、前述した第1実施形態と同様の手順でホスト200Aはドライブ100Aに対してアクセスしているが、そのアクセスに先立ち、ドライブ100A側でホスト200Aの認証を以下のような手順[ステップ(C1)~(C7)]で行なっている。ホスト認証後に、ホスト200Aからドライブ100A(保存部150)に対するコンテンツデータの書き込みは、第1実施形態と同様の手順[ステップ(C8)~(C18)]で行なわれる。なお、図7および図8においては、ステップ(C1)~(C18)に対応する処理を行なっている箇所に、それぞれ(C1)~(C18)が符号として記入されている。

【0078】(C1)ホスト200Aがドライブ100Aにアクセスした際、そのドライブ100A(1回書き込み可能記憶領域160)が何も書き込まれていない初期状態であるか否かを認識し、初期状態である場合、ホストIDを、ROM220から読み出し、ホスト200Aからドライブ100Aへ転送する(図6の転送手段264の機能)。

【0079】(C2)ステップ(C1)でホスト200Aからドライブ100Aへ送られてきたホストIDを1回書き込み可能記憶領域160に書き込み保持する。このとき、記憶領域160に書き込まれたホストIDを、以降、ホストID-1と表記する。

(C3)上述したステップ(C1)および(C2)を実行した後、もしくは、ステップ(C1)でドライブ100Aが初期状態ではないと認識された場合、ホスト200Aは、ドライブ100Aに対してホスト認証を依頼する。

【0080】(C4)ホスト200Aからホスト認証の依頼を受けたドライブ100Aにおいては、乱数発生手段170で乱数を発生し、その乱数をホスト200Aへ送るとともに(図6の転送手段144の機能)、ドライブ100Aからホスト200Aに対し、ホストIDを上記乱数により暗号化したものを転送するように要求する。また、暗号化手段133が、乱数発生手段170で生成された乱数により、記憶領域160に書き込まれているホストID-1を暗号化する。

【0081】(C5)ステップ(C4)の要求に応じて、暗号化手段248が、ROM220に保持されているホストID（このホストIDを、以降、ホストID-2と標記する）を、ドライブ100Aからの乱数により暗号化する。そして、暗号化されたホストID-2をホスト200Aからドライブ100Aへ転送する（図6の転送手段265の機能）。

【0082】(C6)そして、ドライブ100Aの比較判断手段180において、ステップ(C4)で得られた暗号化ホストID-1と、ホスト200Aからの暗号化されたホストID-2とを比較し、これらが一致するか否かを判断する。第2実施形態では、ステップ(C1)および(C2)により初期状態のドライブ100Aの記憶領域160にホストID-1が書き込まれた後は、ホスト200Aやそれ以外のホストがドライブ100Aにアクセスする都度、ドライブ100Aにおいて、記憶領域160に書き込まれたホストID-1に基づき、ホスト認証が行なわれる。

【0083】(C7)ステップ(C6)で一致しないと判断された場合には、ホスト認証に失敗したものと判断し、処理を中断する。ステップ(C6)で一致したと判断された場合には、ホスト200Aの認証に成功したものと判断し、第1実施形態と同様にして、ホスト200Aからドライブ100A（保存部150）に対するコンテンツデータの書き込みが行なわれる。なお、以下のステップ(C8)～(C18)はそれぞれ第1実施形態のステップ(A1)～(A11)に対応している。

【0084】(C8)ホスト200Aからドライブ100Aに対して、ドライブ100A内のROM110領域に保存されている共通鍵群（複数のメディアキーブロック、複数の秘密鍵）および第1ドライブID（静的なID）の転送を要求する。(C9)ステップ(A1)の要求に応じて、共通鍵群および第1ドライブIDを、ROM110から読み出し、ドライブ100Aからホスト200Aへ転送する（図6の転送手段141の機能）。

【0085】(C10)ホスト200AのRAM210に、ドライブ100Aからの共通鍵群および第1ドライブIDを格納・保持する。

(C11)ホスト200A側の乱数発生手段230で乱数を発生し、その乱数をドライブ100Aへ送るとともに（図6の転送手段261の機能）、ホスト200Aからドライブ100Aに対して、生の第2ドライブID（動的なID）とその第2ドライブIDを上記乱数により暗号化したものとの転送を要求する。

【0086】(C12)ステップ(C11)の要求に応じて、暗号化手段131および132が、第2ドライブIDを、ホスト200Aからの乱数と、隠れ領域120に書き込まれているドライブ鍵（秘密鍵）とにより暗号化する。そして、生の第2ドライブIDと暗号化された第2ドライブIDとをドライブ100Aからホスト200Aへ転送

する（図6の転送手段141、142の機能）。

【0087】(C13)ホスト200Aにおいて、暗号化手段242が、ステップ(C10)で保存した共通鍵群と第1ドライブIDとに基づきドライブ鍵（相当）を作成し、そのドライブ鍵とステップ(C11)で生成した乱数とにより、ドライブ100Aからの生の第2ドライブIDを暗号化する。そして、比較判断手段250において、ホスト200A側で暗号化された第2ドライブIDと、ドライブ100Aからの暗号化された第2ドライブIDとを比較し、これらが一致するか否かを判断する。第1実施形態では、上記ステップ(C8)～(C13)により、ドライブ100Aの認証が行なわれる。

【0088】(C14)ステップ(C13)で一致したと判断された場合には、ドライブ100Aの認証に成功したものと判断し、暗号化手段242および244～246が、ROM220から読み出されたホストIDと、RAM210に保存されている共通鍵群および第1ドライブIDとにより、コンテンツ鍵を暗号化する。つまり、ホストIDと共通鍵群とから生成されたホスト鍵と、第1ドライブIDと共通鍵群とから生成されたドライブ鍵（相当）とによって、コンテンツ鍵が暗号化される。

【0089】(C15)ステップ(C14)で暗号化されたコンテンツ鍵を、ホスト200Aからドライブ100Aへ転送し（図1の転送手段262の機能）、ドライブ100Aの保存部150（鍵ファイル151）に書き込む。

(C16)ステップ(C13)で一致したと判断された場合、上述したステップ(C14)、(C15)の処理と並行して、暗号化手段247が、ドライブ100に書き込むべきコンテンツデータをコンテンツ鍵により暗号化する。

【0090】(C17)ステップ(C16)で暗号化されたコンテンツデータを、ホスト200Aからドライブ100Aへ転送し（図1の転送手段263の機能）、ドライブ100Aの保存部150（データファイル152）に書き込む。

(C18)ステップ(C13)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したステップ(C14)～(C17)の処理を行なうことなく、処理を中断する。

【0091】一方、上述のごとくドライブ100Aの保存部150に書き込まれたコンテンツデータをドライブ100Aからホスト200Aへ読み出す際、第2実施形態では、上述と同様のステップ(C1)～(C7)に従ってホスト200Aの認証をドライブ100A側で行ない、さらに、上述と同様のステップ(C8)～(C13)に従ってドライブ100Aの認証をホスト200A側で行なった後、以下のような手順〔ステップ(D1)～(D5)〕でコンテンツデータが読み出される。

【0092】なお、図9および図10においては、ステップ(C1)～(C13)および(D1)～(D4)に対応する処理を行なっている箇所に、それぞれ(C1)～(C13)および(D1)～

(D4)が符号として記入されている。ここで、ステップ(C1)～(C7)によるホスト認証手順およびステップ(C8)～(C13)によるドライブ認証手順は、上述と同様であるので、その説明は省略する。なお、以下のステップ(D1)～(D5)はそれぞれ第1実施形態のステップ(B1)～(B5)に対応している。

【0093】(D1)ステップ(C13)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ホスト200Aは、ドライブ100Aに対し、暗号化コンテンツ鍵および暗号化コンテンツデータの読出を要求する。

(D2)ステップ(D1)の要求に応じて、ドライブ100Aは、暗号化コンテンツ鍵および暗号化コンテンツを保存部150から読み出してホスト200Aへ転送する(図6の転送手段143の機能)。

【0094】(D3)ホスト200Aにおいては、復号化手段271および272が、ROM220から読み出されたホストIDと、RAM210に保存されている共通鍵群および第1ドライブIDとにより、ドライブ100Aの保存部150(鍵ファイル151)から読み出された暗号化コンテンツ鍵を復号化する。つまり、ホストIDと共通鍵群とから生成されたホスト鍵と、第1ドライブIDと共通鍵群とから生成されたドライブ鍵(相当)とによって、暗号化されたコンテンツ鍵が復号化される。

【0095】(D4)そして、復号化手段273が、復号化手段271および272で復号化されたコンテンツ鍵により、ドライブ100Aの保存部150(データファイル152)から読み出された暗号化コンテンツデータを復号化する。

(D5)ステップ(C13)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したステップ(D1)～(D4)の処理を行なうことなく、処理を中断する。

【0096】このように、本発明の第2実施形態としてのデータ保護システムによれば、ドライブ100Aが初期状態である時にこのドライブ100Aに最初に接続されたホスト200Aの識別情報(ホストID-1)が、ドライブ100Aにおける1回書込可能記憶領域160に書き込まれ、それ以降、その記憶領域160に書き込まれたホストID-1に基づいて、ドライブ100Aにアクセスしたホスト200Aが、当該ドライブ100Aに最初に接続されたホスト200A(正規のホスト)であるかどうかの認証が行なわれる。そして、正規のホスト200Aであると認証された場合のみ、ドライブ100Aに対するアクセス(データ書込/読出)が許可される。

【0097】これにより、ドライブ100A側で極めて簡素な認証処理を行なうだけで、正規のホスト200A以外のホストはドライブ100Aにアクセスすることができなくなる。従って、ドライブ100A側での処理の

負荷を大きくすることなく、ドライブ100Aのデータを不正なアクセスから保護することができ、ドライブ100A側での不正コピーのみならず、ホスト200A側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【0098】さらに、ドライブ100Aに最初に接続された正規のホスト200Aしかドライブ100Aにアクセスすることができなくなるので、例えばSTBからハードディスクドライブ(データ記録装置)を取り外しSTB以外のシステムで転用するといった、ドライブ100Aの不正転用をも確実に防止することができる。

【0099】なお、第2実施形態のデータ保護システムにおいては、第1実施形態で説明した技術(つまりドライブ100Aに書き込むべきコンテンツ鍵を第1ドライブIDおよびホストIDにより暗号化する技術)も組み込まれている。これにより、例え何らかの手段を用いてホスト認証を不正にくぐり抜けたとしても、正規のホスト200A以外のホストでは、ドライブ100Aから読み出されたコンテンツ鍵を復号化することができず、コンテンツデータを読み出せない。従って、ホスト200A側での成りすまし等によるデータの不正読出しや不正コピーをより確実に防止することができる。

【0100】〔3〕その他

本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。例えば、上述した第2実施形態のデータ保護システムでは、アクセス毎にドライブ100A側でホスト認証を行なう技術と第1実施形態で説明した技術とを組み合わせているが、アクセス毎にドライブ100A側でホスト認証を行なう技術を、通常のCPRMやCPPMと組み合わせてもよい。具体的には、ステップ(C1)～(C7)を実行した後、第2実施形態におけるステップ(C8)～(C18)、(D1)～(D5)に代えて、ステップ(a1)～(a8)、(b1)、(b2)を実行してもよい。この場合でも、第2実施形態と同様の作用効果を十分に得ることができる。

【0101】また、第1実施形態や第2実施形態におけるドライブ認証手法は、上述したステップ(A1)～(A6)やステップ(C8)～(C13)による手法に限定されるものではない。同様に、第2実施形態におけるホスト認証手法も、上述したステップ(C1)～(C7)による手法に限定されるものではない。

【0102】〔4〕付記

(付記1) データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該アクセス装置の記憶領域に予め登録されているアクセス

装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【0103】(付記2) データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置に、コンテンツ鍵により暗号化されたコンテンツデータを書き込むとともに、所定のアクセス装置識別情報と該データ記録装置の記憶領域に予め登録されている共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込むステップと、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとを含むことを特徴とする、データ保護方法。

【0104】(付記3) 該データ記録装置の認証を行なうステップが、該データ記録装置の記憶領域に予め登録されている共通鍵および第1識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置で乱数を発生するステップと、該乱数を該アクセス装置から該データ記録装置へ転送するステップと、該データ記録装置の記憶領域に予め登録されている第2識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該データ記録装置において、該第2識別情報を、該アクセス装置からの前記乱数と該データ記録装置の秘密鍵とにより暗号化するステップと、暗号化された第2識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置において、該第2識別情報を前記の乱数、共通鍵および第1識別情報により暗号化するステップと、該データ記録装置からの前記暗号化された第2識別情報と該アクセス装置で暗号化された第2識別情報とを比較し、一致するか否かを判断するステップとを含み、これらの第2識別情報が一

致すると判断された場合、該データ記録装置が認証されることを特徴とする、付記1または付記2に記載のデータ保護方法。

【0105】(付記4) データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するためのシステムであって、該データ記録装置が、共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、該アクセス装置からの要求に応じて、前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して該アクセス装置へ転送する第1転送手段と、該アクセス装置からの要求に応じて、該第2識別情報を、当該要求とともに該アクセス装置から送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を該アクセス装置へ転送する第2転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるときに、該アクセス装置が、当該アクセス装置のアクセス装置識別情報を保持する第2記憶領域と、前記乱数を発生する第1乱数発生手段と、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段と、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段と、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段と、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化する第3暗号化手段と、該第3暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第5転送手段と、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第4暗号化手段と、該第4暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第6転送手段とをそなえて構成されたことを特徴とする、データ保護システム。

【0106】(付記5) データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するためのシステムであって、該データ記録装置が、共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、該

アクセス装置からの要求に応じて、前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して該アクセス装置へ転送する第1転送手段と、該アクセス装置からの要求に応じて、該第2識別情報を、当該要求とともに該アクセス装置から送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を該アクセス装置へ転送する第2転送手段と、コンテンツ鍵により暗号化されたコンテンツデータと、所定のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵とを予め書き込まれて保存する保存部と、該アクセス装置からの要求に応じて、前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して該アクセス装置へ転送する第3転送手段とをそなえて構成されるとともに、該アクセス装置が、当該アクセス装置のアクセス装置識別情報を保持する第2記憶領域と、前記乱数を発生する第1乱数発生手段と、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段と、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段と、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段と、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第1復号化手段と、該第1復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第2復号化手段とをそなえて構成されたことを特徴とする、データ保護システム。

【0107】（付記6） 共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置であって、当該アクセス装置のアクセス装置識別情報を保持する第2記憶領

域と、前記乱数を発生する第1乱数発生手段と、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段と、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段と、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段と、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化する第3暗号化手段と、該第3暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第5転送手段と、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第4暗号化手段と、該第4暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第6転送手段とをそなえて構成されたことを特徴とする、アクセス装置。

【0108】（付記7） 共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第3転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置であって、当該アクセス装置のアクセス装置識別情報を保持する第2記憶領域と、前記乱数を発生する第1乱数発生手段と、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段と、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段と、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化され



た第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段と、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第1復号化手段と、該第1復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第2復号化手段とをそなえて構成されたことを特徴とする、アクセス装置。

【0109】(付記8) 共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第3転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置であって、当該アクセス装置のアクセス装置識別情報を保持する記憶領域と、前記乱数を発生する第1乱数発生手段と、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段と、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段と、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段と、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化する第3暗号化手段と、該第3暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第5転送手段と、該データ記録装置に記録・保存すべき前記コンテンツデータを、該コンテンツ鍵により暗号化する第4暗号化手段と、該第4暗号化手段により暗号化されたコンテンツデ

ータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第6転送手段と、前記の第2識別情報が一致すると該第1比較判断手段が判断した場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第1復号化手段と、該第1復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第2復号化手段とをそなえて構成されたことを特徴とする、アクセス装置。

【0110】(付記9) 共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムであって、前記乱数を発生する第1乱数発生手段、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化する第3暗号化手段、該第3暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第5転送手段、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第4暗号化手段、および、該第4暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第6転送手段として、該コンピュータを機能させることを特徴とする、アクセスプログラム。

【0111】(付記10) 共通鍵、第1識別情報および

び第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第3転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムであって、前記乱数を発生する第1乱数発生手段、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第1復号化手段、および、該第1復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第2復号化手段として、該コンピュータを機能させることを特徴とする、アクセスプログラム。

【0112】（付記11） 共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムを記録したコンピュ

ータ読取可能な記録媒体であって、該アクセスプログラムが、前記乱数を発生する第1乱数発生手段、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出された前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するか否かを判断する第1比較判断手段、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化する第3暗号化手段、該第3暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第5転送手段、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第4暗号化手段、および、該第4暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第6転送手段として、該コンピュータを機能させることを特徴とする、アクセスプログラムを記録したコンピュータ読取可能な記録媒体。

【0113】（付記12） 共通鍵、第1識別情報および第2識別情報を保持する第1記憶領域と、外部からの要求に応じて前記の共通鍵、第1識別情報および第2識別情報のうちの少なくとも一つを該第1記憶領域から読み出して要求元へ転送する第1転送手段と、外部からの要求に応じて、該第2識別情報を、当該要求とともに送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第1暗号化手段と、該第1暗号化手段により暗号化された第2識別情報を要求元へ転送する第2転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第3転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムを記録したコンピュータ読取可能な記録媒体であって、該アクセスプログラムが、前記乱数を発生する第1乱数発生手段、該第1乱数発生手段で発生された該乱数を該データ記録装置へ転送する第4転送手段、該データ記録装置の該第1記憶領域から読み出された該第2識別情報を、該第1乱数発生手段で発生された該乱数と、該データ記録装置の該第1記憶領域から読み出され

た前記の共通鍵および第1識別情報とにより暗号化する第2暗号化手段、該データ記録装置からの前記暗号化された第2識別情報と該第2暗号化手段で暗号化された第2識別情報とを比較し、一致するかどうかを判断する第1比較判断手段、これらの第2識別情報が一致すると該第1比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第1識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第1復号化手段、および、該第1復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第2復号化手段として、該コンピュータを機能させることを特徴とする、アクセスプログラムを記録したコンピュータ読取可能な記録媒体。

【0114】(付記13) データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、1回のみ書き込み可能な記憶領域に書き込むステップと、以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記1回のみ書き込み可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報によりコンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【0115】(付記14) 該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報により、前

記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとをさらに含むことを特徴とする、付記13記載のデータ保護方法。

【0116】(付記15) データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、1回のみ書き込み可能な記憶領域に書き込むステップと、以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記1回のみ書き込み可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、コンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【0117】(付記16) 該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第1識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとをさらに含むことを特徴とする、付記15記載のデータ保護方法。

【0118】(付記17) 該アクセス装置の認証を行なうステップが、該データ記録装置で乱数を発生するステップと、該乱数を該データ記録装置から該アクセス装

置へ転送するステップと、該データ記録装置において、該アクセス装置識別情報を前記乱数により暗号化するステップと、該アクセス装置において、該アクセス装置識別情報を該データ記録装置からの前記乱数により暗号化するステップと、暗号化された該アクセス装置識別情報を該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置からの前記暗号化されたアクセス装置識別情報と該データ記録装置で暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断するステップとを含み、これらのアクセス装置識別情報が一致すると判断された場合、該アクセス装置が認証されることを特徴とする、付記13～付記16のいずれか一つに記載のデータ保護方法。

【0119】(付記18) 該データ記録装置の認証を行なうステップが、該データ記録装置の記憶領域に予め登録されている共通鍵および第1識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置で乱数を発生するステップと、該乱数を該アクセス装置から該データ記録装置へ転送するステップと、該データ記録装置の記憶領域に予め登録されている第2識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該データ記録装置において、該第2識別情報を、該アクセス装置からの前記乱数と該データ記録装置の秘密鍵とにより暗号化するステップと、暗号化された第2識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置において、該第2識別情報を前記の乱数、共通鍵および第1識別情報により暗号化するステップと、該データ記録装置からの前記暗号化された第2識別情報と該アクセス装置で暗号化された第2識別情報とを比較し、一致するか否かを判断するステップとを含み、これらの第2識別情報が一致すると判断された場合、該データ記録装置が認証されることを特徴とする、付記13～付記17のいずれか一つに記載のデータ保護方法。

【0120】(付記19) 該データ記録装置が、初期状態の時に最初に接続された該アクセス装置のアクセス装置識別情報を書き込まれる、1回のみ書込可能な記憶領域と、該アクセス装置からアクセスされる都度、該データ記録装置で乱数を発生する第2乱数発生手段と、該第2乱数発生手段で発生された該乱数を該アクセス装置へ転送する第7転送手段と、前記1回のみ書込可能な記憶領域から読み出された該アクセス装置識別情報を、該第2乱数発生手段で発生された該乱数により暗号化する第5暗号化手段と、該第5暗号化手段で暗号化されたアクセス装置識別情報と、該アクセス装置からの、該乱数により暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断する第2比較判断手段とをさらにそなえとともに、該アクセス装置が、初期状態の該データ記録装置に最初に接続された時に、該アクセス装置識別情報を該第2記憶領域から読み出して該データ記録

装置へ転送する第8転送手段と、該アクセス装置識別情報を、該データ記録装置から送られてくる乱数により暗号化する第6暗号化手段と、該データ記録装置にアクセスする都度、該第6暗号化手段により暗号化されたアクセス装置識別情報を該データ記録装置へ転送する第9転送手段とをさらにそなえ、該第1比較判断手段および該第2比較判断手段がいずれも識別情報が一致すると判断した場合で且つコンテンツデータを該データ記録装置に記録・保存する場合に、該第3暗号化手段、該第5転送手段、該第4暗号化手段および該第6転送手段が動作することを特徴とする、付記4記載のデータ保護システム。

【0121】(付記20) 該データ記録装置が、該アクセス装置からの要求に応じて、前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して該アクセス装置へ転送する第3転送手段をさらにそなえて構成されるとともに、該アクセス装置が、該第1比較判断手段および該第2比較判断手段がいずれも識別情報が一致すると判断した場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該第2記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第1識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第1復号化手段と、該第1復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第2復号化手段とをそなえて構成されたことを特徴とする、付記19記載のデータ保護システム。

【0122】(付記21) データを記録・保存し、アクセス装置からのアクセスに応じて該データの書込/読出を行なうデータ記録装置であって、初期状態の時に最初に接続された該アクセス装置のアクセス装置識別情報を書き込まれる、1回のみ書込可能な記憶領域と、該アクセス装置からアクセスされる都度、該データ記録装置で乱数を発生する第2乱数発生手段と、該第2乱数発生手段で発生された該乱数を該アクセス装置へ転送する第7転送手段と、前記1回のみ書込可能な記憶領域から読み出された該アクセス装置識別情報を、該第2乱数発生手段で発生された該乱数により暗号化する第5暗号化手段と、該第5暗号化手段で暗号化されたアクセス装置識別情報と、該アクセス装置からの、該乱数により暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断する第2比較判断手段とをそなえて構成されたことを特徴とする、データ記録装置。

【0123】

【発明の効果】以上詳述したように、本発明のデータ保護方法(請求項1, 2)によれば、アクセス装置(ホスト)がコンテンツデータおよびコンテンツ鍵をデータ記録装置に書き込む際に、コンテンツ鍵が、データ記録装

置の識別情報にアクセス装置識別情報（ホストID）の要素を加えて暗号化されているので、コンテンツデータやコンテンツ鍵をデータ記録装置に書き込んだ正規のアクセス装置しか、そのコンテンツデータを読み出すことができない。つまり、正規のアクセス装置以外のアクセス装置がデータ記録装置からコンテンツデータを読み出しても、そのアクセス装置の識別情報が正規のものと異なっているため、コンテンツ鍵を正しく復号化することができないので、コンテンツデータを正しく復号化できず、コンテンツデータを読み出すことができなくなる。従って、ＣＰＰＭやＣＰＲＭ等の単方向認証を採用してデータ記録装置側での処理の負荷を大きくすることなく、データ記録装置のデータを不正なアクセスから保護することができ、データ記録装置側での不正コピーのみならず、アクセス装置側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【0124】また、本発明のデータ保護方法（請求項3～5）によれば、データ記録装置（ドライブ）が初期状態である時にこのデータ記録装置に最初に接続されたアクセス装置（ホスト）の識別情報（ホストID）が、データ記録装置における1回のみ書込可能な記憶領域に書き込まれ、それ以降、その記憶領域に書き込まれた識別情報に基づいて、データ記録装置にアクセスしたアクセス装置が、当該データ記録装置に最初に接続されたアクセス装置（正規のアクセス装置）であるかどうかの認証が行なわれる。そして、正規のアクセス装置であると認証された場合のみ、データ記録装置に対するアクセス（データ書込／読出）が許可される。

【0125】これにより、データ記録装置側で極めて簡単な認証処理を行なうだけで、正規のアクセス装置以外のアクセス装置はデータ記録装置にアクセスすることができなくなる。従って、データ記録装置側での処理の負荷を大きくすることなく、データ記録装置のデータを不正なアクセスから保護することができ、データ記録装置側での不正コピーのみならず、アクセス装置側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【0126】さらに、データ記録装置に最初に接続された正規のアクセス装置しかデータ記録装置にアクセスすることができなくなるので、例えばセットトップボックスからハードディスクドライブ（データ記録装置）を取り外しセットトップボックス以外のシステムで転用するといった、データ記録装置の不正転用をも確実に防止することができる。

【0127】なお、最初に接続されたアクセス装置の識別情報をデータ記録装置における1回のみ書込可能な記憶領域に書き込みその識別情報を用いてアクセス装置の認証を行なう技術と、データ記録装置に書き込むべきコンテンツ鍵をデータ記録装置識別情報およびアクセス装

置識別情報により暗号化する技術とを組み合わせることにより、例え何らかの手段を用いてアクセス装置の認証を不正にくぐり抜けたとしても、正規のアクセス装置以外のアクセス装置では、データ記録装置から読み出されたコンテンツ鍵を復号化することができず、コンテンツデータを読み出せない。従って、アクセス装置側での成りすまし等によるデータの不正読出しや不正コピーをより確実に防止することができる。

【図面の簡単な説明】

【図1】本発明の第1実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図である。

【図2】第1実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図である。

【図3】第1実施形態におけるコンテンツデータ書込手順を説明するための図である。

【図4】第1実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図である。

【図5】第1実施形態におけるコンテンツデータ読出手順を説明するための図である。

【図6】本発明の第2実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図である。

【図7】第2実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図である。

【図8】第2実施形態におけるコンテンツデータ書込手順を説明するための図である。

【図9】第2実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図である。

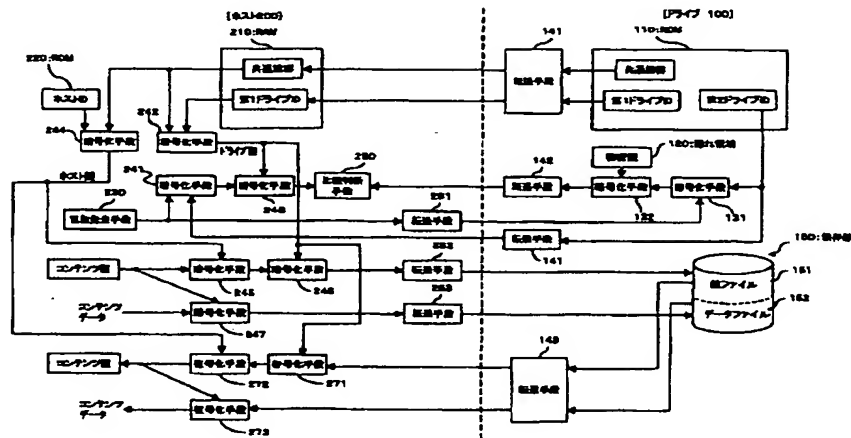
【図10】第2実施形態におけるコンテンツデータ読出手順を説明するための図である。

【符号の説明】

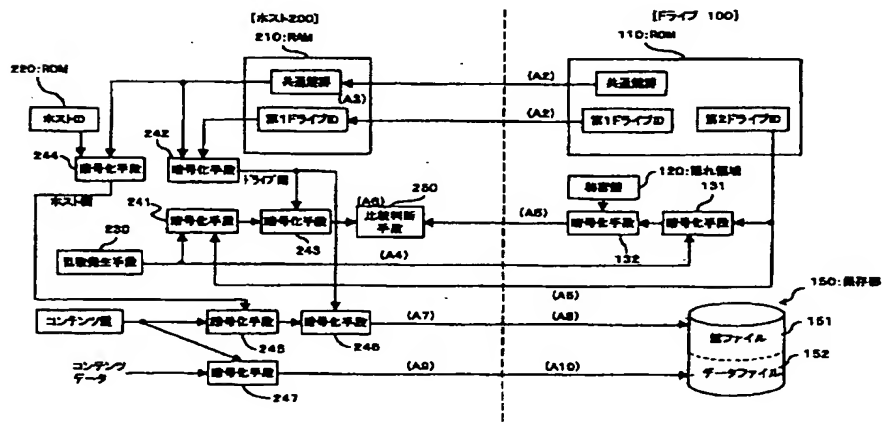
- 100、100A ドライブ（データ記録装置）
- 110 ROM（第1記憶領域）
- 120 隠れ領域
- 131、132 暗号化手段（第1暗号化手段）
- 133 暗号化手段（第5暗号化手段）
- 141 転送手段（第1転送手段）
- 142 転送手段（第2転送手段）
- 143 転送手段（第3転送手段）
- 144 転送手段（第7転送手段）
- 150 保存部
- 151 鍵ファイル
- 152 データファイル
- 160 1回書込可能記憶領域
- 170 乱数発生手段（第2乱数発生手段）

- |                               |                          |
|-------------------------------|--------------------------|
| 180 比較判断手段 (第2比較判断手段)         | 247 暗号化手段 (第4暗号化手段)      |
| 200, 200A ホスト (アクセス装置)        | 248 暗号化手段 (第6暗号化手段)      |
| 210 RAM                       | 250 比較判断手段 (第1比較判断手段)    |
| 220 ROM (第2記憶領域)              | 261 転送手段 (第4転送手段)        |
| 230 乱数発生手段 (第1乱数発生手段)         | 262 転送手段 (第5転送手段)        |
| 241, 243 暗号化手段 (第2暗号化手段)      | 263 転送手段 (第6転送手段)        |
| 242 暗号化手段 (第2暗号化手段, 第3暗号化手段)  | 264 転送手段 (第8転送手段)        |
| 244, 245, 246 暗号化手段 (第3暗号化手段) | 265 転送手段 (第9転送手段)        |
|                               | 271, 272 復号化手段 (第1復号化手段) |
|                               | 273 復号化手段 (第2復号化手段)      |

【図1】

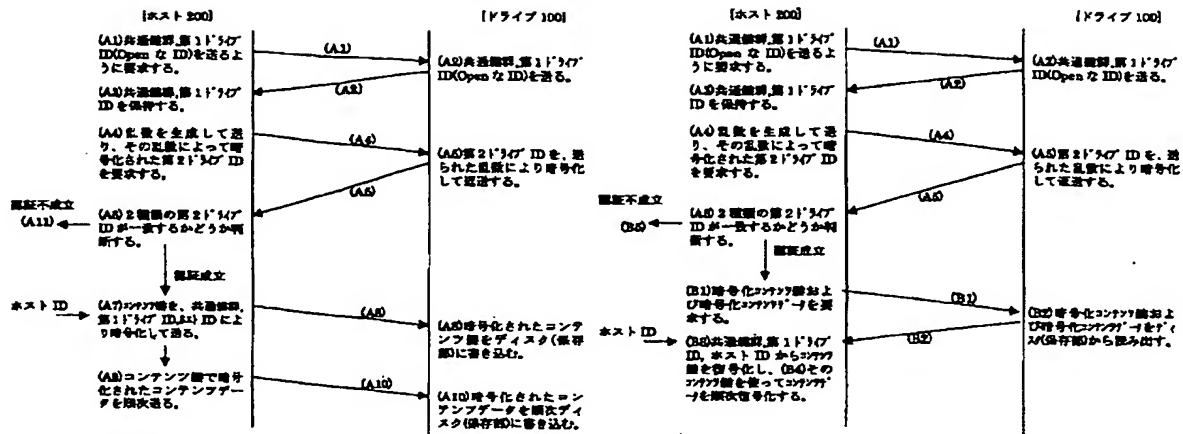


【図2】

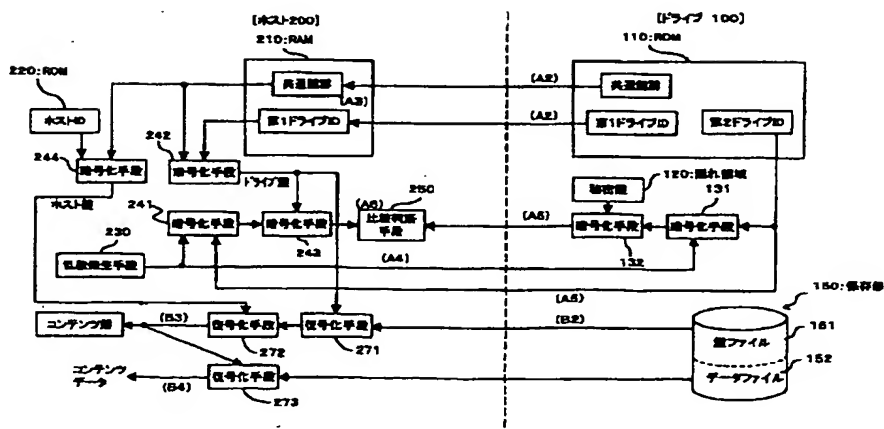




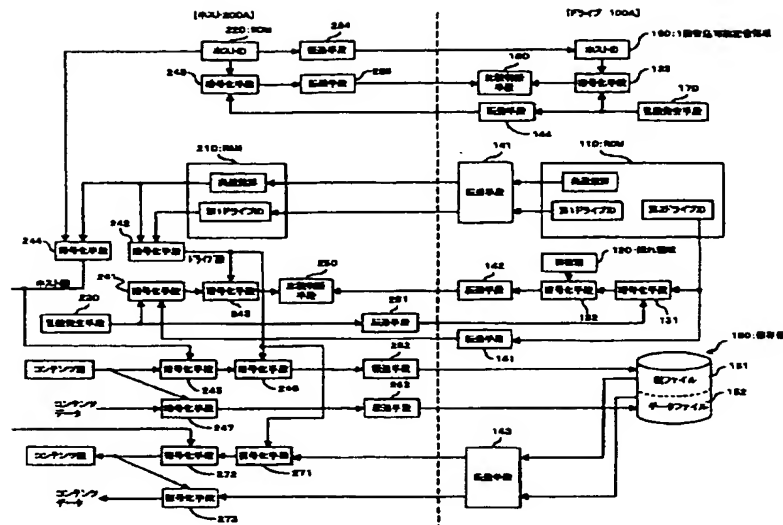
【图5】



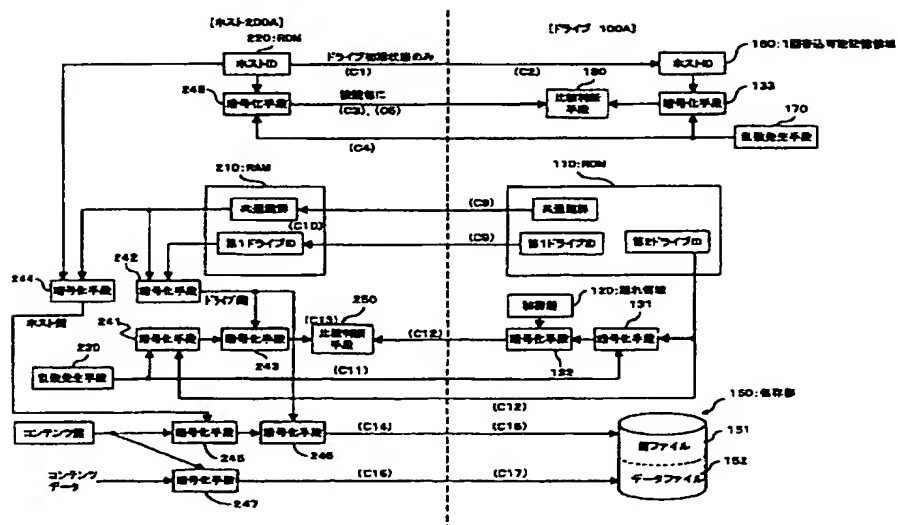
【图4】



【図6】



【図7】



```

graph TD
    subgraph Host_Path [Host ID Path]
        C1H["(C1) 近接状態でのホスト ID を得る。  
(C2) ホスト ID を検索する。"]
        C3H["(C3) 得られた近接によりホスト ID を時号化して送る。"]
        C4H["(C4) 近接状態時、第1'の ID IDmax を ID とする。"]
        C5H["(C5) 近接状態時、第1'の ID ID を得る。"]
        C6H["(C6) ID を生成して送り、その近接によって時号化された第2'の ID ID を要求する。"]
        C7H["(C7) ID を近接の第2'の ID ID が一致するかどうか検知する。"]
        C8H["(C8) ID を近接状態時、第1'の ID IDmax を ID とする。"]
        C9H["(C9) ID を生成して送り、その近接によって時号化されたコンテンツデータを要求する。"]
        C10H["(C10) コンテンツデータで時号化されたコンテンツデータを伝送する。"]
    end

    subgraph Device_Path [Device ID Path]
        C1D["(C1) 近接状態では ID に接続されたホストの ID を、1 個のみを ID みに可能に書き込む。"]
        C2D["(C2) ID を生成して送り、その近接により時号化されたホスト ID を要求する。ホスト ID-1 を近接により時号化する。"]
        C3D["(C3) 近接状態時、第1'の ID ID と時号化された ID とが一致するかどうか検知する。"]
        C4D["(C4) 近接状態時、第1'の ID IDmax を ID とする。"]
        C5D["(C5) 第2'の ID ID を、得られた近接により時号化して伝送する。"]
        C6D["(C6) 時号化されたコンテンツデータをディスタック保存部に書き込む。"]
        C7D["(C7) 時号化されたコンテンツデータをディスタック保存部に書き込む。"]
    end

    Host_Path --> Device_Path
    Device_Path --> Host_Path
  
```

Figure 1 is a flowchart illustrating the ID assignment process. The process is divided into two main sections: Host ID and Device ID. The Host ID section (left) starts with (C1) obtaining the host ID in the proximity state, followed by (C2) searching for the host ID. (C3) involves sending the obtained proximity ID, and (C4) involves using the first ID as the ID. (C5) involves obtaining the first ID, and (C6) involves sending the ID and requesting the second ID. (C7) involves checking if the IDs match, and (C8) involves using the first ID as the ID. (C9) involves sending the ID and requesting the content data, and (C10) involves transmitting the content data. The Device ID section (right) starts with (C1) writing the host ID to the proximity state, followed by (C2) sending the ID and requesting the host ID. (C3) involves checking if the IDs match, and (C4) involves using the first ID as the ID. (C5) involves sending the second ID, and (C6) involves writing the content data to the distastack storage unit. (C7) involves writing the content data to the distastack storage unit. The flowchart shows the interaction between the Host ID and Device ID sections, with arrows indicating the sequence of steps and the flow of data.

Figure 1 is a block diagram of a data processing system. The system is divided into two main sections by a dashed line. The left section (ROM 200) includes a ROM 200, a CPU 201, a RAM 210, and various control units (C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13). It also features a display unit 240, a keyboard unit 241, and a printer unit 242. The right section (ROM 100A) includes a ROM 100A, a CPU 101, a RAM 110, and various control units (C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13). It also features a display unit 140, a keyboard unit 141, and a printer unit 142. The system is connected to a database 150 via a network 151 and 152.

```

graph TD
    subgraph Host_300A [ホスト 300A]
        C1[初期状態の時のホスト ID を送る。]
        C2[ホスト ID 照会の依頼を送る。]
        C3[送られた仮数によりホスト ID を等号化し返す。]
        C4[角度無効、第 1 "ラフ ID" IDpass を ID を送る。]
        C5[角度無効、第 1 "ラフ ID" ID を保持する。]
        C6[仮数を生じて送り、その仮数によって等号化された第 2 "ラフ ID" ID を返す。]
        C7[第 2 照会の第 2 "ラフ ID" が一致するかどうかが判明する。]
        C8[等号化コソング番号および等号化コソング ID を返す。]
        C9[角度無効、第 1 "ラフ ID" ID、ホスト ID からコソング ID を等号化し、C10 そのコソング ID を受けてコソング ID を角度無効等号化する。]
    end

    subgraph Drive_300A [ドライブ 300A]
        D1[初期状態時で最初に送られたホストの ID を、1 回のみを送込み可算領域に書き込む。]
        D2[仮数を生じて送り、その仮数により等号化された ID ID を返す。]
        D3[等号化した ID ID と等号化ホスト ID ID とが一致するかどうかが判明する。]
        D4[角度無効、第 1 "ラフ ID" IDpass を ID を送る。]
        D5[角度無効、第 1 "ラフ ID" ID を保持する。]
        D6[第 2 "ラフ ID" ID を、送られた仮数により等号化して返す。]
        D7[等号化コソング番号および等号化コソング ID が一致するかどうかが判明する。]
    end

    C1 --> D1
    C2 --> D2
    C3 --> D3
    C4 --> D4
    C5 --> D5
    C6 --> D6
    C7 --> D7
    C8 --> D8
    C9 --> D9
  
```

Figure 1 is a flowchart illustrating the first embodiment of the invention. The process involves a Host 300A and a Drive 300A. The Host 300A sends an initial ID and a request for a file. The Drive 300A checks if the file is in the cache, database, or backup. If found, it returns the file. If not, it generates a temporary ID and returns it. The Host 300A then checks if the temporary ID matches the requested ID. If yes, it returns the file. If no, it generates a new ID and returns it. The Drive 300A then checks if the new ID matches the requested ID. If yes, it returns the file. If no, it returns an error.

Fターム(参考) 5B017 AA06 AA07 BA07 BA09 CA15  
5B065 BA01 CA17 CC08 CS06 PA04  
PA16  
5J104 AA01 AA07 AA16 EA04 EA17  
JA03 NA02 PA14